AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America
v.
BRAIDEN CAROLL WILLIAMS

Case No. 3-22-mj-70962MAG

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 2, 2022 to April 26, 2022 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
Title 18, USC § 371	Conspire to commit any offense against the United States Maximum sentence: Five years custody, $250,000 fine, three years supervised release, $100 special assessment.

This criminal complaint is based on these facts:

See Affidavit.

☑ Continued on the attached sheet.

/s/ J.F.S.
Complainant's signature

Approved as to form __/s_____
AUSA H. G.

FBI Special Agent J.F.S.
Printed name and title

Sworn to before me by telephone.

Date: 07/22/2022

Judge's signature

City and state: San Francisco, CA

Alex G. Tse, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANT AND CRIMINAL COMPLAINT

I. INTRODUCTION AND AGENT BACKGROUND

I, J. F. S.,[1] being duly sworn, state as follows:

1. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7).

2. I am employed as a Special Agent with the Federal Bureau of Investigation ("FBI") in Kansas City, Missouri and have been so employed since 2019. I am sworn and empowered to investigate criminal activity involving violations of federal law. I am currently assigned to FBI's Kansas City Cyber Crimes Task Force, which investigates crimes carried out using computers or computer networks. I have participated in numerous interviews of witnesses and have been the affiant of federal search warrants involving suspected criminal violations where records, of the type involved in this investigation, were seized. My investigative experience includes, but is not limited to interviewing subjects, targets, and witnesses; executing search and arrest warrants; handling and supervising confidential human sources; conducting surveillance; and analyzing phone records and financial records.

3. This affidavit is made in support of an application for a criminal complaint and arrest warrant for BRAIDEN CAROLL WILLIAMS ("WILLIAMS"). For the reasons set forth below, and based on my training, experience, and familiarity with WILLIAMS and this investigation, I submit that there is probable cause to believe that WILLIAMS is involved in a conspiracy to violate 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing a computer without authorization and thereby obtain information from a protected computer, in violation of 18 U.S.C. § 371.

[1] Your affiant seeks to use initials throughout the affidavit and complaint due to Williams's involvement in online threats. Williams has potentially been linked to additional prior swatting incidents and his associates have been linked to swatting of a U.S. law enforcement officers.

4. The facts set forth in this affidavit are based on information that I have obtained from my personal involvement in the investigation and from other law enforcement officers who have been involved in this investigation (including special agents of the Internal Revenue Service and United States Secret Service). This affidavit does not set forth all of my knowledge about this matter; it is intended to only show that there is sufficient probable cause for the requested warrant and criminal complaint.

II. APPLICABLE STATUTES

5. Title 18, Section 371, makes it a crime for two or more persons to conspire either to commit any offense against the United States or to defraud the United States.

6. Title 18, United States Code, Section 1030(a)(2)(C), in relevant part, makes it a crime for an individual to intentionally access a computer without authorization, or exceeding authorized access, and thereby obtain information from a protected computer. Under Section 1030(c)(2)(B), the offense is a felony if "committed for purposes of commercial advantage or private financial gain," "committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," or if "the value of the information obtained exceeds $5,000." A "protected computer" means a computer that is used in or affecting interstate or foreign commerce or communication (as defined by 18 U.S.C. § 1030(e)(2)(B)).

III. DEFINITIONS

7. I know from my training and experience as a Special Agent with the FBI that the following definitions apply to the activity discussed in this affidavit:

8. **Bitcoin**: Bitcoin is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

9. **Cryptocurrency exchangers**: Exchangers are persons or entities in the business of exchanging fiat currency (currency that derives its value from government regulation or law, such as the U.S. dollar) for cryptocurrency, and exchanging cryptocurrency for fiat currency. When a user wishes to purchase cryptocurrency from an exchanger, the user will typically send payment in the form of fiat or other convertible virtual currency to an exchanger, usually via wire or ACH, for the corresponding number of cryptocurrency based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell cryptocurrency, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed. Based on my training and experience, cryptocurrency exchanges send confirmation emails to the email account used to register the member exchange account for each deposit, trade, and/or withdraw cryptocurrency and fiat transactions conducted by the user on the exchange.

10. **Cryptocurrency wallet**: A cryptocurrency wallet is an application that holds a user's cryptocurrency addresses and private keys. A cryptocurrency wallet also typically allows users to send, receive, and store cryptocurrency. Different cryptocurrency wallets support different types of cryptocurrencies.

11. **SIM swapping**: SIM swapping is a type of account takeover fraud that generally targets weaknesses in authentication mechanisms targeting mobile telephones, allowing criminals to take over a victim's telephone and its communications. Cyber criminals will generally change the SIM card associated with a victim's account and/or telephone number with a SIM card the criminal controls. Once the SIM card is changed, the criminal controls the victim's telephone number, which then can be used to reset accounts containing valuable property (such as cryptocurrency accounts) or other valuable information. Many online accounts are secured with authentication features that rely on the user controlling a particular mobile telephone number, so once a victim's telephone number has been taken over by one of the perpetrators, the perpetrators can take over the accounts that they are targeting.

12. **Swatting**: Swatting is the act of illegally calling law enforcement to report a false emergency at a target location with the intent to create a tactical response by law enforcement. Individuals will often "swat" others to seek revenge for a grievance or to instill fear in others, which has resulted in multiple deaths across the United States where law enforcement mistakenly shot and killed innocent people after false information was reported.

IV. FACTS ESTABLISHING PROBABLE CAUSE IN SUPPORT OF THE ARREST WARRANT AND CRIMINAL COMPLAINT

Overview of Email Hijacking and SIM Swapping Resulting in Theft of Cryptocurrency and of This Conspiracy

13. Based on my training and experience and through knowledge gained investigating SIM swaps and related criminal activity, I know it is common practice to conduct email hijacking and SIM swaps to fraudulently access and steal from cryptocurrency or other financial accounts as part of a team. The various roles necessary to conduct an email hijack, SIM swap, and subsequent theft of cryptocurrency or bank account funds may be referred to differently depending on the group or actors involved but include at a minimum a "Searcher," a "Holder," and a "Caller." The first step in these criminal operations is usually to access a target's email account without authorization, which is commonly referred to as hijacking the target's email account. The Searcher is typically the individual who hijacks a victim's email account and searches through the victim's email to determine whether he or she has financial or cryptocurrency accounts of a high enough value worth trying to steal. Searchers may also conduct public searches to find potential victims who hold cryptocurrency and/or exploit aspects of certain cryptocurrency exchanges.[2] Searchers use different tools to hijack victim's email accounts, including brute force techniques (basically employing computer scripts against the email account to run many passwords against the account

[2] For example, some exchanges require higher levels of authentication for accounts containing cryptocurrency worth over a certain dollar amount. By knowing the levels of authentication required, criminal actors can assess the value of a particular target's account by probing the account with account reset requests, which they are then able to view because they have hijacked a victim's email account.

to see if one permits access to the account), and the use of leaked or purchased databases containing personally identifiable information and sometimes passwords for accounts. The Holder is the individual who has the SIM card and cell phone to which the victim account will be swapped. The Caller is the individual who contacts the telecom company with whom the victim has cell phone service and initiates the SIM swap from the victim's device to the Holder's device. Once the victim's service has been swapped to the Holder's device, the Holder provides the two-factor authentication codes to the Searcher who then uses the codes to access the victim's financial accounts and/or cryptocurrency accounts and steals their money and/or cryptocurrency. The Searcher is able to do this because he or she is already able to access the victim's email account, and then is able to receive (through the Holder) any pin codes needed for two-factor authentication, which typically are delivered to the victim through text message, email, or authentication app, all of which the criminal actors have access to following the email hijacking and SIM swap of the victim's email account and phone. Actors may serve multiple roles but I have found, based on my investigation of SIM swapping, that these actors rarely work alone when conducting SIM swaps because each role is demanding and the actors typically attempt to victimize multiple targets at once.

14. There is probable cause to believe that WILLIAMS and others are involved in a conspiracy to steal cryptocurrency from victims using SIM swaps. Specifically, there is evidence that this group of co-conspirators first hijacked victims' email accounts and then conducted reconnaissance on potential victims by trying to fraudulently initiate password resets for victims' Coinbase accounts.[3] After identifying victims who were likely to have higher amounts of

[3] Coinbase is a cryptocurrency exchange where account holders can buy, sell, transfer, and store cryptocurrency. Coinbase controls wallets that store user's cryptocurrency. Coinbase offers online accounts that can be access via the Internet, and users can transact via their online accounts. Coinbase users have the option to secure their accounts using multi-factor authentication. For example, a user can require that logging into his or her account requires both a password as well as a second level of authentication through a pin code provided to his or her mobile phone, email, or other two-factor authentication application. By taking over

cryptocurrency in their accounts, WILLIAMS and/or his co-conspirators performed SIM swaps on these victims, resulting in control of victims' cellular telephone numbers. With this control, WILLIAMS and/or his co-conspirators then were able to access without authorization victims' Coinbase accounts that typically require multi-factor authentication. Specifically, WILLIAMS and his co-conspirators were able to log into a victims' Coinbase account by resetting the victim's Coinbase password, and then entering the pin code provided by Coinbase to do so, which is typically provided by Coinbase to the victim via text message, email, or other two-factor authentication application. Once they had access to victims' Coinbase accounts, WILLIAMS and/or his co-conspirators transferred victims' cryptocurrency out of their accounts into accounts controlled by WILLIAMS and/or his co-conspirators. Additionally, at least two victims reported that their email accounts were compromised and that whoever did so may have attempted to conceal their unauthorized access to the victims' email accounts by blocking future emails from Coinbase for one victim, presumably so the victim would not see emails from Coinbase showing funds transferred out of his account, and by moving all new emails for another victim in the email account's trash folder, to accomplish the same concealment.

15. As alleged below, WILLIAMS and/or his co-conspirators committed a variety of acts in furtherance of the alleged conspiracy, including acts in the Northern District of California.

April 2022 SIM Swapping and Crypto Theft Victims

16. On April 5, 2022, Victim 1, a resident of Farmington, Minnesota, reported to the Farmington Police Department (FPD) that during the evening of April 3, 2022 or the morning of April 4, 2022, he was the victim of a theft from his Coinbase account and had lost approximately $153,000. Victim 1 subsequently reported his Verizon cell phone number had been SIM swapped to a new device sometime in the late evening of April 3, 2022, without his authorization and

someone else's Coinbase account, a perpetrator of SIM swapping can transfer cryptocurrency out of that account for their own gain.

criminal actors then appeared to use the SIM swapped phone number to gain access to his Coinbase account and steal his funds. Victim 1's Verizon account was under his father's name, and at approximately 11:15 pm CDT on April 3, 2022, Victim 1's father received an email from Verizon regarding a transfer request for a phone number ending in the same last four digits as Victim 1's phone number. The settings for Victim 1's email account, which was linked to his Coinbase account, had also been changed without his authorization to include Coinbase as a blocked domain. This change blocked Coinbase emails from arriving in Victim 1's email account. I believe that this was done to avoid having Victim 1 see any emails from Coinbase that would have shown transfers of cryptocurrency out of his account and any additional notification about possible compromise of his Coinbase account.

17. Through legal process, FPD obtained records from Verizon indicating activity for Victim 1's phone number on two devices from April 3 to April 4, 2022. I have reviewed these records. The first device was Victim 1's iPhone 7, and the second device was an unknown iPhone 7 with IMEI 354911096564653 ("Holder Device"). The Verizon records also indicated that beginning on April 3, 2022, at approximately 10:41 PM CDT, and ending around April 4, 2022, at approximately 1:30 AM CDT, data activity for Victim 1's phone number was being routed through the eNodeB ID 136702.[4] Verizon provided the specific latitude and longitude coordinates for eNodeB 136702 as 29.431272/-98.477553 and the address as 811 N. Alamo, San Antonio, Texas, 78215.

18. In addition to Verizon records, FPD obtained records from Apple for data associated with the Holder Device. I have reviewed these records. The records indicated the billing profile for the iCloud account with email address 14@live.ca was linked to the Holder Device on March 23, 2022. The iCloud account with email address 14@live.ca is subscribed to WILLIAMS. Apple records show that the Holder Device was last activated with a cellular provider

[4] An eNodeB is a mobile (cellular) base station used in 4G-LTE compliant Mobile Networks, which provides the wireless connectivity between the network and user device.

on March 28, 2022. Apple records then show that on April 4, 2022, (at approximately 10:46 pm CDT), Victim 1's phone number was activated on the Holder Device. The iCloud account with email address 14@live.ca, subscribed to WILLIAMS, was used to sign onto the Holder Device's iTunes Music Store on April 9, 2022, and was used to update the Holder Device on April 16, 2022. From April 2, 2022 to April 26, 2022, 30 different phone numbers (including Victim 1's phone number) were activated on the Holder Device. In my training and experience, this volume of different phone numbers being activated on a single device is consistent with use of the device as a Holder's device to conduct fraudulent SIM swaps.

19. T-Mobile records related to the Holder Device indicated that on or about April 3, 2022, 8 customer phone numbers were SIM swapped to the Holder Device and in the month of April 2022, a total of 25 customer phone numbers were SIM swapped to the Holder Device. Two of the T-Mobile customers whose accounts were SIM swapped to the Holder Device submitted complaints to the FBI's Internet Crime Complaint Center, known as IC3. The first victim (Victim 2) reported a loss of approximately $30,000 from his Coinbase account and the second victim (Victim 3) reported a loss of approximately $200,000 from his Coinbase account. In their IC3 complaints, Victim 2 reported having his T-Mobile phone SIM swapped on or about April 3, 2022, and Victim 3 reported having his T-Mobile phone SIM swapped on or about April 4, 2022, each prior to the reported crypto theft from their respective Coinbase accounts. Victim 2 also reported that during this time, his email account (which was linked to his Coinbase account), was also compromised. He reported that he later discovered that whoever compromised his email account had moved all new email messages to the Trash folder. Therefore, although Victim 2 had access to his email account during the SIM swap and theft of his Coinbase cryptocurrency, he did not see the multiple emails sent from Coinbase to his email account about unauthorized transfers of cryptocurrency out of his Coinbase account.

20. Another of the eight T-Mobile customers whose account was SIM swapped to the Holder Device on April 3, 2022, (Victim 4) resided in San Jose, California, which is in the

Northern District of California. Victim 4 was in San Jose, California when the SIM swap occurred. According to Victim 4, he suffered no financial loss because he had secured his cryptocurrency accounts with more than just two-factor authentication through his cell phone. However, Victim 4 reported that he did need to work with T-Mobile in order to regain access to his cell phone account following the SIM swap.

21. FPD obtained records from Coinbase for Victim 1's compromised account. I have reviewed these records. These records show that a "password reset request" was performed in the early morning hours of April 3, 2021, from IP address 172.249.146.127 (".127 IP address").

22. Based on records provided from Charter Communications, the .127 IP address resolves to an individual with initials M.R with a residential address located in Fullerton, CA.[5]

23. Based on my training and experience, I know individuals engaged in SIM swapping and crypto theft often perform reconnaissance on numerous potential victim accounts by attempting password resets prior to SIM swapping a selected victim and accessing his or her account. I know that, for example, Coinbase responds differently to account password reset requests based on, for example, the security settings in a customer's account and the amount of cryptocurrency in a customer's account. I also know that actors engaged in SIM swapping are aware of the different responses Coinbase can send for a password reset request and use these different responses to determine which accounts to target for crypto theft.

24. Additional Coinbase records for account information related to .127 IP address indicated that the .127 IP address was associated with 9 additional Coinbase accounts[6] on April 3, 2022. One of the individuals whose account was accessed on April 3, 2022, from the .127 IP address (Victim 5) is a resident of the Northern District of California. Victim 5 only had

[5] The full name and address of this subscriber were provided by Charter Communications and are known to me.

[6] Each of the account holders for the 9 additional Coinbase accounts accessed from the .127 IP address were distinct from the 8 account holders whose T-Mobile accounts were SIM swapped to the Holder Device.

approximately $300 in her Coinbase account, did not recall ever being the victim of a SIM swap, and upon review did not have any cryptocurrency stolen from her account.

Evidence Linking WILLIAMS to Conspiracy

25. As noted above, WILLIAMS is the subscriber listed for iCloud account with email address 14@live.ca, which was linked to the Holder Device before and during some of the SIM swaps to the Holder Device noted above.

26. As noted above, during the time that Victim 1's cellular phone was SIM swapped to the Holder Device, Victim 1's phone number was being routed through an eNodeB that resolved to a longitude and latitude located at 811 N. Alamo, San Antonio, TX. 78215. During this same time period, from March 17, 2022 to April 17, 2022, WILLIAMS had rented housing through Airbnb located at 319 East Jones Avenue, Unit 8, San Antonio, Texas, 78215, which is approximately 2.7 miles from the eNodeB which Victim 1's phone number was routed through during the SIM swap.

27. On or about July 21, 2022, FBI agents conducted a voluntary interview of Braiden WILLIAMS. During the interview WILLIAMS admitted to the following:

a. WILLIAMS was lived in San Antonio, Texas at 319 East Jones Avenue, Unit 8, San Antonio, TX 78215 and 2510 W. Woodlawn Ave, San Antonio, TX 78228 from approximately the middle of March until the middle of June.

b. While residing at the above listed addresses, WILLIAMS participated in multiple SIM swaps of victim phones to a device that he controlled.

c. During this time, WILLIAMS worked as a Holder for a group of individuals who referred to themselves as "ACG." WILLIAMS stated that one or more individuals acted as Callers.

d. The SIM swaps that WILLIAMS assisted with resulted in the theft of cryptocurrency from victim accounts.

e. In exchange for WILLIAMS's work as a Holder for the various SIM swaps, he was paid in Bitcoin by members of ACG.

f. WILLIAMS used an Exodus wallet to store his Bitcoin.[7] He claimed that the highest value he had on his Exodus wallet at one time was cryptocurrency worth approximately $114,000.

g. WILLIAMS cashed out the Bitcoin he received and used the proceeds to fund travel to Europe and to purchase three vehicles: an orange 2020 Dodge Challenger, a black 2015 Ford Mustang, and a 2016 Dodge Challenger.

h. WILLIAMS's iCloud account was tied to the email address 14@live.ca and he as the only person who had access to that iCloud account.

Summation of April 2022 Conspiracy

28. Given the nature of these criminal actors, the manner in which they perform their criminal activity, and the information presented above, I believe that on or about April 3, 2022, a co-conspirator using the .127 IP address to access at least ten Coinbase accounts, including those of Victim 1 and Victim 5, who is based in the Northern District of California, with the intent to perform fraudulent SIM swaps and steal the victim's cryptocurrency. After identifying targets who were likely to have higher levels of cryptocurrency in their accounts, this co-conspirator and possibly others worked with WILLIAMS to perform SIM swaps of at least 30 victims in the month of April 2022.

29. Throughout the course of this conspiracy to defraud these victims, WILLIAMS served as the Holder and received the victims' cell phone service to the Holder Device, which he controlled. These included SIM swaps of Victim 1, Victim 2, Victim 3, and Victim 4. Victim 4 was located in the Northern District of California when the SIM swap occurred. Once WILLIAMS received the victims' cell phone service, either WILLIAMS or a co-conspirator used two-factor authentication codes meant for the victim but sent to the Holder Device to attempt to gain access to the victims' cryptocurrency accounts and steal their funds.

[7] Exodus is a type of cryptocurrency wallet that allows users to send, receive, and exchange over 225 different types of cryptocurrencies, including Bitcoin.

30. In the case of Victim 1, Victim 2, and Victim 3, the actions of WILLIAMS and his co-conspirators resulted in the theft of cryptocurrency from their Coinbase accounts, resulting in losses totaling approximately $380,000.

V. CONCLUSION AND REQUEST FOR SEALING

31. Based on the above information, along with my training and experience, I respectfully submit that there is probable cause to believe that WILLIAMS , as well as others known and unknown, conspired to commit a crime against the United States, specifically, violations of 18 U.S.C. § 1030(a)(2)(C), all in violation of 18 U.S.C. § 371.

32. Since this investigation is ongoing, disclosure of the Application, Affidavit, Warrant, and Order and the attachments thereto will jeopardize the investigation by apprising the subjects of the existence of the investigation and providing subjects an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court seal the Application, Affidavit, and Warrant and Order and all attachments, until further Order of this Court, except that the clerk of the Court provide copies to representatives of the United States Attorney's Office, the Federal Bureau of Investigations, and the United States Marshal Service for use in this case, which can be provided to other United States Attorney's Office, the Federal Bureau of Investigations, and any other law enforcement agencies both federal or local, necessary to investigate and prosecute this case, and execute the Arrest Warrant.

/s/ J.F.S. by AGT

J.F.S.
Special Agent
Federal Bureau of Investigation

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) on this 22nd day of July, 2022. This application and warrant are to be filed under seal.

HONORABLE ALEX G. TSE
United States Magistrate Judge